

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

| | | |
|---------------------------|---|--------------------|
| UNITED STATES OF AMERICA, |) | |
| |) | |
| Plaintiff, |) | |
| |) | No. 3:08-CR-142 |
| V. |) | |
| |) | (PHILLIPS/SHIRLEY) |
| DAVID C. KERNELL, |) | |
| |) | |
| Defendant. |) | |

MEMORANDUM AND ORDER

All pretrial motions in this case have been referred to the undersigned pursuant to 28 U.S.C. § 636(b) for disposition or report and recommendation regarding disposition by the District Court as may be appropriate. This cause is before the Court on Defendant Kernell's Renewed and Amended Motion for Bill of Particulars [Doc. 46]. The parties came before the Court on June 30, 2009, for a motion hearing on the pending motions. Assistant United States Attorneys D. Gregory Weddle, Mark L. Krotoski, and Josh Goldfoot appeared on behalf of the Government, and Attorneys Wade V. Davies and Anne E. Passino appeared on behalf of the Defendant, who was also present. At the conclusion of his arguments on his motion for a bill of particulars, the Defendant requested the opportunity to file a supplemental brief. The Court granted this request. The Defendant filed a Supplement to Motion for Bill of Particulars [Doc. 58] on July 6, 2009. The Government responded [Doc. 62] on July 13, 2009.

The Defendant asks the Court to order the Government to provide a bill of particulars identifying the following:

With regard to the Introductory Allegations,

- (1) The manner in which the Defendant is alleged to have falsely represented his identity in paragraph 7;
- (2) The other individual(s) who is/are alleged to have accessed the email account in paragraph 12;

With regard to Count 1,

- (3) The use in and affect on interstate commerce;
- (4) The source of the “lawful authority” governing the means of identification;

With regard to Count 2,

- (5) The records and files in question in paragraph 25;
- (6) The electronic transmission in paragraph 26;
- (7) The Yahoo! computers in paragraph 26;

With regard to Count 3,

- (8) The computer the Defendant is alleged to have accessed without authorization;
- (9) The “protected computer” from which the Defendant is alleged to have obtained information;
- (10) The information obtained by the Defendant from the protected computer;
- (11) The individuals whom the Defendant is alleged to have aided and abetted;
- (12) Which type of invasion of privacy action is alleged; and

With regard to Count 4,

(13) Which record or document is alleged to have been altered, destroyed, or concealed and the approximate time.

The Defendant contends that knowledge of these details is necessary for him to prepare his defense, to avoid unfair surprise at trial, and to permit him to avoid a future double jeopardy violation. He argues that the Government is obligated to particularize the charges so that it might properly plead its case. Such particularization inevitably involves the disclosure of evidence and legal theories.

The Government responds that the Superseding Indictment clearly and fully informs the Defendant of the charges and the specific conduct forming the bases therefor. It contends, moreover, that it has provided the Defendant with extensive discovery that reveals the prosecution's case in detail. It argues that the Defendant's request for a bill of particulars improperly seeks to discover evidentiary details or the Government's legal theories.

Federal Rule of Criminal Procedure 7(f) states that

[t]he court may direct the government to file a bill of particulars. The defendant may move for a bill of particulars before or within 10 days after arraignment or at a later time if the court permits. The government may amend a bill of particulars subject to such conditions as justice requires.

“A bill of particulars is meant to be used as a tool to minimize surprise and assist defendant in obtaining the information needed to prepare a defense and to preclude a second prosecution for the same crimes. It is not meant as a tool for the defense to obtain detailed disclosure of all evidence held by the government before trial.” United States v. Salisbury, 983 F.2d 1369, 1375 (6th Cir. 1993). The granting of a bill of particulars is within the court's discretion. See id. (holding that the appellate court reviews the denial of a bill of particulars for an abuse of discretion). The level of detail in the indictment can be a basis for denying the motion for a bill of particulars. Id. Additionally, “a defendant is not entitled to a bill of particulars with respect to information which

is available through other sources.” United States v. Paulino, 935 F.2d 739, 750 (6th Cir. 1991), superseded on other grounds by stat., United States v. Caseslorete, 220 F.3d 727 (6th Cir. 2000) (on sentencing issue). Guided by these principles, the Court turns to the Defendant’s requests.

(1) Particularization of Introductory Allegations

The Defendant requests particularization of paragraphs 7 and 12 of the Introductory Allegations in the Superseding Indictment. Paragraph 7 states that “[i]n resetting the password to the email account gov.palin@yahoo.com, defendant KERNELL falsely represented his identity as the account holder of the e-mail account and concealed his true identity.” The Defendant asks that the Government specify the manner in which he is alleged to have falsely represented his identity in this paragraph. The Court finds that the information the Defendant seeks is contained within paragraph 7: The Defendant is alleged to have falsely represented his identity by holding himself out as the email’s account holder and concealing his true identity. The Court finds that no further particularization is necessary.

With regard to paragraph 12, the Defendant asks the Government to identify the other individuals who are alleged to have accessed Governor Palin’s email account. Paragraph 12 states as follows:

Defendant KERNELL also posted the reset password and provided others with the means of access to the e-mail account, including confidential and personal information in the account. At least one other individual successfully used the reset password to access the gov.palin@yahoo.com email account.

At the hearing, the Defendant argued that knowing the identity of these individuals was critical to his understanding of Count 3, which charges him with aiding and abetting other violations of 18

U.S.C. § 1030. The Government stated that it had provided the Defendant with IP logs showing the IP addresses of the individuals who accessed Governor Palin's account after the Defendant accessed it as well as subscriber information for those IP addresses. The Court finds that the Government has also sufficiently identified the other individuals who are alleged to have accessed Governor Palin's email account.

(2) Count 1

Count 1 charges the Defendant with identity theft as follows:

On or about September 16, 2008, in the Eastern District of Tennessee, and elsewhere, defendant

DAVID C. KERNELL,

did knowingly transfer, possess, and use in and affecting interstate and foreign commerce, without lawful authority, a means of identification of another person, that is, the Yahoo! ID and date of birth of Governor Sarah Palin, with the intent to commit, and to aid or abet, and in connection with, any unlawful activity that constitutes a violation of Federal law, that is, Fraud and Related Activity in Connection with Computers, under 18 U.S.C. § 1030(a)(2)(C), and Wire Fraud, under 18 U.S.C. § 1343.

The Defendant asks for particularization of how the means of identification was used in and affected interstate commerce and the source of "lawful authority" governing the means of identification.

This Court has already found [Doc. 89]¹ that the Superseding Indictment sufficiently charges the affect on interstate commerce in Count 1:

In the present case, the Court finds that the allegations in the Superseding Indictment show that the actions alleged in Counts 1 and

¹The Court notes that the Defendant did not file an objection to this Report and Recommendation.

3 affected interstate commerce. The introductory allegations in the indictment, which are expressly incorporated in Counts 1 and 3, state that the defendant was living in Tennessee and that Yahoo! is a California corporation, which provides e-mail services throughout the United States. The Indictment also alleges that Yahoo!'s computers and servers were located outside of Tennessee. The individual whose computer the defendant is alleged to have accessed was the Governor of Alaska. In light of these allegations that span at least three states, the Court cannot say as a matter of law that the charges fail to allege the jurisdictional element.

Accordingly, the Court determines that additional particularization is not necessary.

With regard to the "lawful authority" alleged in Count 1, paragraph 8 of the Superseding Indictment alleges that "[a]t no time did defendant KERNELL have authorization from Governor Palin to access and use the e-mail account gov.palin@yahoo.com." The Court finds that no additional specification of this allegation is required.

(3) Particularization of Count 2

Count 2 charges the Defendant with wire fraud as follows:

On or about September 16, 2008, in the Eastern District of Tennessee and elsewhere, defendant KERNELL did knowingly devise, and intend to devise, a scheme and artifice to defraud, and for obtaining property, that is, information data and pictures from the e-mail account gov.palin@yahoo.com, by means of material false and fraudulent pretenses, representations, and promises, and the concealment of material facts. . . . defendant

DAVID C. KERNELL,

for the purpose of executing and attempting to execute the above-described scheme and artifice to defraud, and for obtaining property, did knowingly transmit, and cause to be transmitted, and aided and abetted the transmission of an electronic transmission between the defendant's computer in Knoxville, Tennessee and Yahoo! computers located outside the State of Tennessee.

The Defendant moves for particularization of the records and files that he is alleged to have “removed, altered, concealed and covered up on his computer concerning his involvement in the scheme” to defraud. He also requests that the Government identify the specific electronic transmissions that constituted the wire fraud and the specific Yahoo! computers alleged in the offense.

With regard to the computer data the Defendant is alleged to have deleted, paragraph 25 of Count 2 expressly identifies that as “records and files on his laptop computer concerning his involvement in the scheme.” At the hearing, the Government stated that the specific files alleged to have been destroyed or deleted are identified with great specificity in the forensic report setting out the results of the search of the Defendant’s computer. The Court’s own review of that report in conjunction with the Defendant’s suppression motions confirms this statement. Additionally, AUSA Weddle stated that the Government is alleging that the Defendant’s Facebook account was deleted and that it had provided the Defendant with information regarding the deletion of the Facebook account. The Court finds that the records and files in question have been sufficiently particularized.

The Defendant contends that identification of the electronic transmission or transmissions is essential because this information makes up the primary element of wire fraud. He asserts that this case involves numerous electronic transmissions. At the hearing, the Government argued that it had provided the Defendant with the IP logs showing the various times that the Defendant was logged onto Governor Palin’s email account and his transmissions with Yahoo! in advance of accessing Palin’s account. It contended that the subsequent transmissions of information from her account to others were also relevant to the wire fraud count.

The Court finds that the Government is alleging that the electronic transmissions at issue are those between the Defendant's computer and Yahoo!, between the Defendant's computer and Governor Palin's Yahoo! email account, and between the Defendant and others conveying information from Governor Palin's Yahoo! email account. Although the Government maintains that the Defendant can deduce which transmissions are the subject of the wire fraud count, in light of the number of transmissions and the difference in recipients, the Court finds that particularization of the electronic transmissions that form the basis of Count 2 is appropriate so that the Defendant can prepare to defend this count at trial.

Finally, with regard to Count 2, the Defendant asks that the Government identify the specific Yahoo! computer or computers that received the electronic transmissions. Count 2 states that the Yahoo! computers are located outside of Tennessee. The Court finds that unlike the specific electronic transmissions at issue, knowledge of the specific computer or computers is not necessary for the Defendant to prepare his defense.

(4) Particularization of Count 3

Count 3 charges the Defendant with the unauthorized access of a protected computer in furtherance of another crime or tort:

The introductory allegations set forth in paragraphs 1 - 14 are re-alleged herein. On or about September 16, 2008, in the Eastern District of Tennessee and elsewhere, defendant

DAVID C. KERNELL,

in furtherance of the commission of a criminal and tortious act in violation of the laws of the United States and the State of Tennessee, including aiding and abetting other violations of 18 U.S.C. § 1030(a)(2)(C) (Fraud and Related Activity in Connection with

Computers); and tortious invasion of privacy, intentionally and without authorization, and in excess of authorization, accessed a protected computer by means of an interstate communication and thereby obtained information, and did aid and abet in same.

The Defendant asks the Court to order the Government to particularize five aspects of this charge: (1) the computer he allegedly accessed without authorization, (2) the “protected computer” from which he allegedly obtained information, (3) the information allegedly obtained, (4) the individuals whom he allegedly aided and abetted, and (5) the type of invasion of privacy that is alleged. The Court’s analysis thus far speaks to numbers (1), (2), and (4). The “protected” computer accessed was a Yahoo! computer or computers located outside of Tennessee. The identity of which actual Yahoo! computer was involved is not necessary. Additionally, the Government has provided the IP addresses and subscriber information of the other individuals, and no additional particularization is needed.

With regard to the information the Defendant allegedly obtained from the protected computer, paragraph 10 of the Introductory Allegations, which are expressly incorporated in Count 3, states as follows:

The confidential and personal information included, and was not limited to, other email addresses of her family members, pictures of her family members, at least one cell phone number of her family member, the dates of birth of Governor Palin and another member of her family, and Governor Palin’s address book for her Yahoo! email account.

The Court observes that this list does not purport to be comprehensive. It also notes that forensic report detailing the results of the searches of the Defendant’s computer list this information in detail. If the Government contends that the information obtained contains something that does not come within the categories listed in paragraph 10, then it must particularize what that is.

Finally, the Defendant asks for particularization of the type of invasion of privacy alleged in Count 3. In his Memorandum in Support of Motion to Dismiss Computer Fraud Count and Its Felony Enhancement, the Defendant states that “[i]n Tennessee, a civil cause of action is available for invasion of privacy, but Tennessee only recognizes a cause of action for intrusion upon seclusion and publicly placing a person in a false light.” [Doc. 40, p.9 (footnotes omitted)] At the hearing, the Government responded that it was “not alleging an invasion of privacy action. We are . . . alleging a tortious act of invasion of privacy under Tennessee law, and those acts are described in the indictment.” AUSA Weddle contended that anything beyond what was alleged in the indictment would amount to the Government’s legal theory regarding the invasion of privacy tort, the disclosure of which was not an appropriate reason for particularization.

The Court finds that although the Government does not have to prove all of the elements of the tort of invasion of privacy in order to prove a tortious act, knowledge of the type of invasion of privacy at issue is necessary for the Defendant to prepare his defense. Accordingly, the Court orders that the Government particularize the type of Tennessee invasion of privacy of which the alleged tortious act is an element.

(5) Particularization of Count 4

Count 4 charges the Defendant with the anticipatory obstruction of justice as follows:

Between on or about September 16, 2008, and on or about September 20, 2008, in the Eastern District of Tennessee, and elsewhere, defendant

DAVID C. KERNELL

did knowingly alter, destroy, and conceal a record and document with the intent to impede, obstruct and influence an investigation of a

matter by, and within the jurisdiction of, the Federal Bureau of Investigation, and in relation to and contemplation of such a federal investigation.

The Defendant requests particularization of the records or documents that he has alleged to have altered, destroyed or concealed and the approximate time of such action. As discussed above with regard to Count 2, the Government stated that the specific files alleged to have been destroyed or deleted are identified with great specificity in the forensic report setting out the results of the search of the Defendant's computer. AUSA Weddle stated that "[e]verything that we contend was altered, deleted or modified is contained within either the computer forensic reports, which have been provided, it is detailed almost file by file what we say [was] deleted and when it was deleted." Second, AUSA Weddle stated that the items deleted included the Defendant's Facebook account and that information regarding the deletion of the Facebook account. The Court finds that the records and documents in question have been sufficiently particularized.

CONCLUSION

Accordingly, the Defendant's Renewed and Amended Motion for Bill of Particulars [**Doc. 46**] is **GRANTED in part** in that the Government is **ORDERED** to provide a bill of particulars:

- (1) Identifying the electronic transmissions alleged in Count 2;
- (2) Specifying any information obtained from the protected computer in Count 3 in addition to that listed in paragraph 10 of the Superseding Indictment; and
- (3) particularizing the type of Tennessee invasion of privacy alleged in Count 3,

and is **DENIED in all other respects**. The Government is **ORDERED** to provide the bill of particulars on or before **April 9, 2010**.

IT IS SO ORDERED.

ENTER:

s/ C. Clifford Shirley, Jr.
United States Magistrate Judge